個資內部稽核管理
教育訓練

課程大綱

- 個人資訊管理系統(PIMS)稽核
- 執行個資管理稽核
- 驗證稽核案例分享
- 矯正與預防程序

Tutor
講師

個人資訊管理系統(PIMS)稽核

9 Performance evaluation 績效評估

- **9.1 Monitoring, measurement, analysis and evaluation監督、量測、分析及評估**
- **9.2 Internal audit 內部稽核**
- **9.3 Management review管理審查**

內部稽核

9.2 Internal audit 內部稽核

組織應採取下列作為：

1) 規劃、建立、實作及維持稽核計畫，包括頻率、方法、責任、規劃要求事項及報告。該稽核計畫應將所關注之重要過程及前次稽核之結果納入考量；
2) 定義稽核之準則及稽核之範圍；
3) 選擇稽核員及施行稽核，以確保稽核過程之客觀性及公平性；
4) 確保稽核之結果對相關管理階層報告；以及
5) 保存文件化資訊作為稽核計畫及稽核結果之證據。

稽核方案應明確包含所有高風險個人資訊(see 8.2.2.2)的相關處理過程，及所有由分包商所執行之個人資訊處理過程(參照 8.2.11.10))

監視、量測、分析與評估規劃

執行項目	監測指標	負責人員	監測週期	監測時間	監測結果	監測人員

執行項目	分析/評估指標	負責人員	分析/評估週期	分析/評估準則	分析/評估結果	分析/評估人員

稽核

Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled.

一為系統化、中立的及文件化過程，取得稽核證據並進行客觀的評估，以確定符合稽核基準的程度。

個人資訊管理系統(PIMS)稽核

ISO 19011:2011 管理系統稽核指導綱要，提供稽核指導包含:

- 稽核原則
- 稽核規劃管理
- 稽核活動
- 稽核員職能

第一者稽核 (內部稽核)

- **定義：**
  - 組織本身針對自我系統及程序的稽核

- **目的：**
  - 確保個人資訊管理系統的維持、發展及改進

- **要求：**
  - BS 10012:2017 9.2 內部稽核

第二者稽核 (外部稽核)

- **定義:**
  - 組織對其供應商、分包商執行的一種稽核

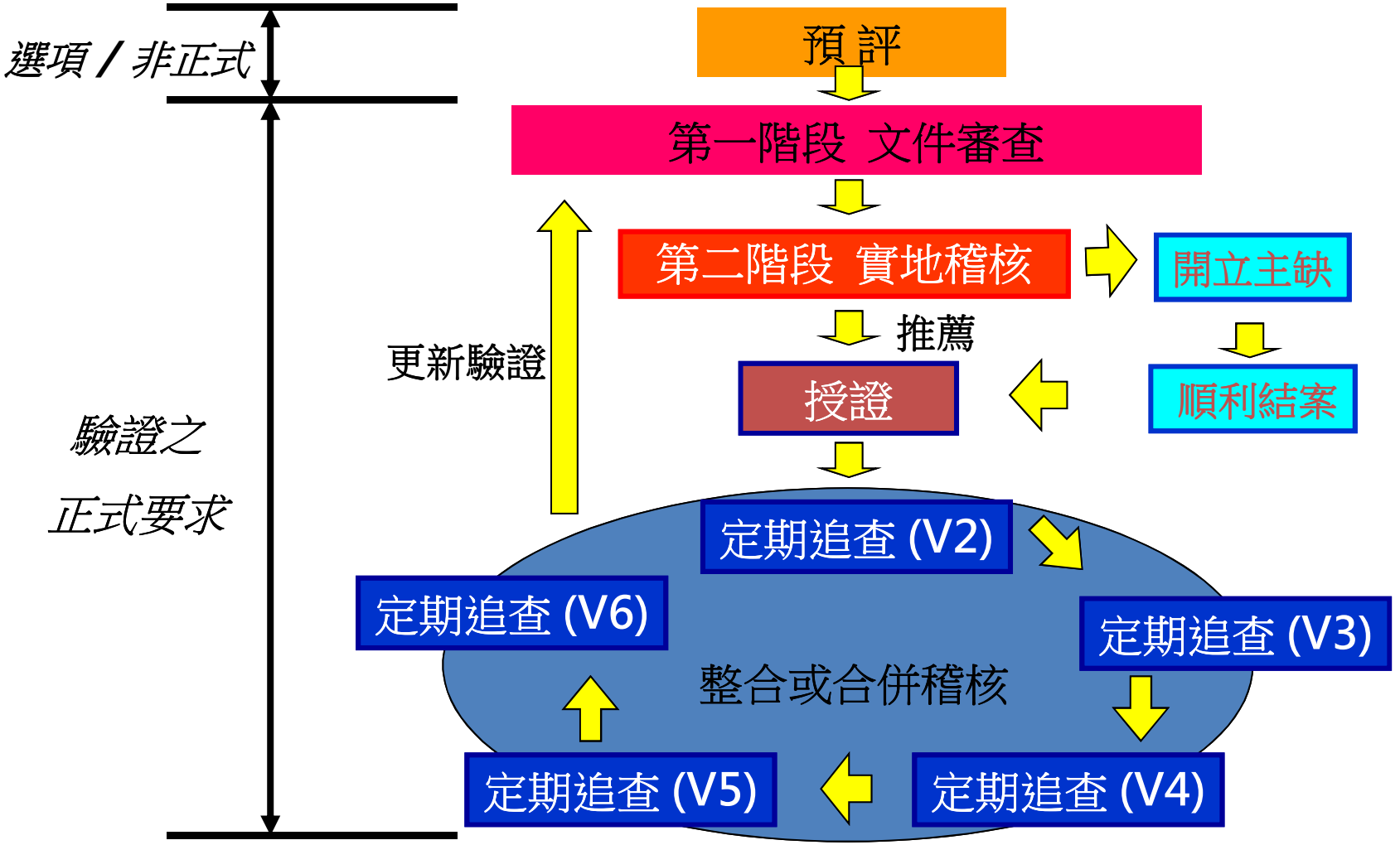
- **目的 :**
  - 決定供應商、分包商的適用性
  - 評核供應商、分包商的績效
  - 確定供應商、分包商的能量

第三者稽核 (外部稽核)

- **定義：**
  - 獨立於組織所執行的稽核
    (例如驗證機構對組織進行BS 10012個人資訊管理系統稽核)

- **目的：**
  - 確定組織是否依據標準建立, 文件化, 執行與維持其個人資訊管理系統

驗證過程


選項 / 非正式
驗證之
正式要求
預 評
第一階段 文件審查
第二階段 實地稽核
開立主缺
推薦
順利結案
授證
更新驗證
定期追查 (V2)
定期追查 (V3)
定期追查 (V4)
定期追查 (V5)
定期追查 (V6)
整合或合併稽核

稽核原則

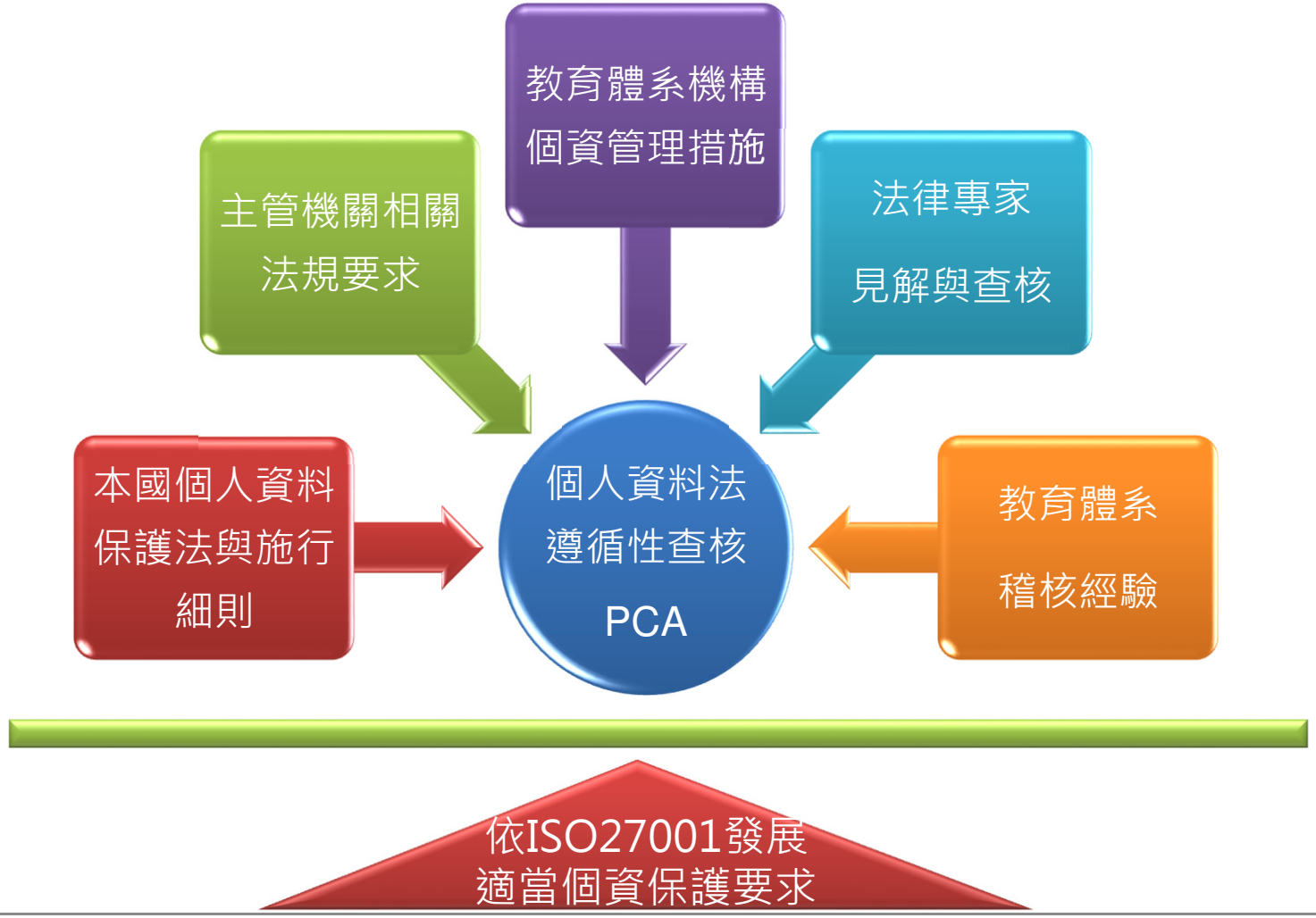
- **與稽核員有關之原則：**
  - 職業操守：專業精神之基礎
  - 公正表現：誠實地與準確地報告之義務
  - 專業應盡之責：稽核時之敬業精神與判斷力

- **與稽核有關之原則：**
  - 獨立性：為稽核時公正無私與稽核結論客觀之基礎
  - 以證據為依據：於系統化的稽核程序中，運用條理的方法使稽核結論具可信度與再現性

稽核員應備職能

- **PIMS terminology 個人資訊管理系統專業術語**
- **product, services and operational processes 產品, 服務與作業過程**
- **organisational situation 組織的現況**
- **risk and security assessments 風險及安全評鑑**
- **personal information management principles 個資保護原則**
- **audit methodology 稽核方法論**
- **legislative, contractual and other relevant requirements 相關法規, 合約與其他的要求**

個資法規遵循性查核(PCA)依據準則



教育體系相關法令

- 個人資料保護法及個人資料保護法施行細則
- 100-102年度教育機構個人資料保護工作事項
- 教育體系個人資料安全保護基本措施
- 私立專科以上學校及私立學術研究機構個人資料檔案安全維護實施辦法
- 大學法/施行細則
- 學位授予法/施行細則
- 私立學校法...

執行個資管理稽核

稽核規劃管理

- 建立稽核之目標與範圍
- 建立責任、資源與程序
- 執行稽核方案
- 監視與審查方案
- 紀錄維護

稽核方案目標與範圍

目標

- 應依據
  - 管理上的優先順序
  - 商業目的
  - 管理系統要求
  - 法令與合約要求
  - 供應商評估
  - 顧客要求
  - 營運風險

範圍

- 範疇與界線描述應包括：
  - 地理位置
  - 組織單位
  - 受稽者活動與流程
  - 稽核期間

稽核方案的範圍與資源

- **範圍受下列影響：**
  - 範圍, 目標, 期間與頻率
  - 組織之規模, 狀態, 重要性, 複雜性與業務活動所在地
  - 標準, 法規、合約要求, 政策及稽核準則
  - 認證/ 驗證要求
  - 先前稽核的結果
  - 語言, 文化, 社會議題
  - 利益團體的考量
  - 組織重大的變更
  - 個別稽核員之職能

- **資源考量：**
  - 財務資源
  - 稽核方式
  - 達成與維持稽核員職能的流程
  - 稽核員與技術專家的可用性
  - 稽核計畫的範圍
  - 差旅時間, 住宿等

稽核準則

- **包括：**
  - 適用的標準
  - 管理系統要求
  - 政策
  - 程序
  - 法規
  - 法令
  - 合約要求
  - 工業/ 產業之行為守則

內部稽核可採行流程

- **年度規劃**
  - 年度稽核計畫
  - 稽核資源安排
  - 各次稽核人選
- **各次稽核作業**
  - 當次稽核計畫
  - 稽核開幕會議
  - 稽核活動執行
  - 稽核結束會議
  - 矯正與預防作業
  - 追蹤與覆核作業

年度稽核計畫

- **排定年度稽核計畫時應考量：**
  - 現有稽核資源
  - 前次個人資訊管理稽核缺失項目追蹤情形
  - 該年度個人資訊管理作業重點項目
- **年度稽核計畫項目安排應考量：**
  - 個人資訊管理系統要求。
  - 個人資訊管理文件要求。
  - 個人資訊管理高風險項目。
  - 個人資訊管理安控措施較難管制項目。
  - 前次稽核發現之缺失。
  - 個人資訊管理安全事件發生頻繁項目。

當次稽核計畫

- **預定實施前提出稽核計畫**
- **涵蓋項目**
  - 當次稽核團隊領隊與成員
  - 查核範圍與受稽單位
  - 查核項目時間安排
- **注意事項**
  - 稽核團隊成員獨立性要求-不能稽核與自身相關的作業
  - 過去個人資訊管理相關稽核結果
  - 必要查核作業項目
  - 應以風險程度為依據安排
- **計畫內容**
  - 目標/範圍 /稽核準則—標準、程序
  - 受稽單位/稽核團隊成員
  - 日期與地點/時程安排

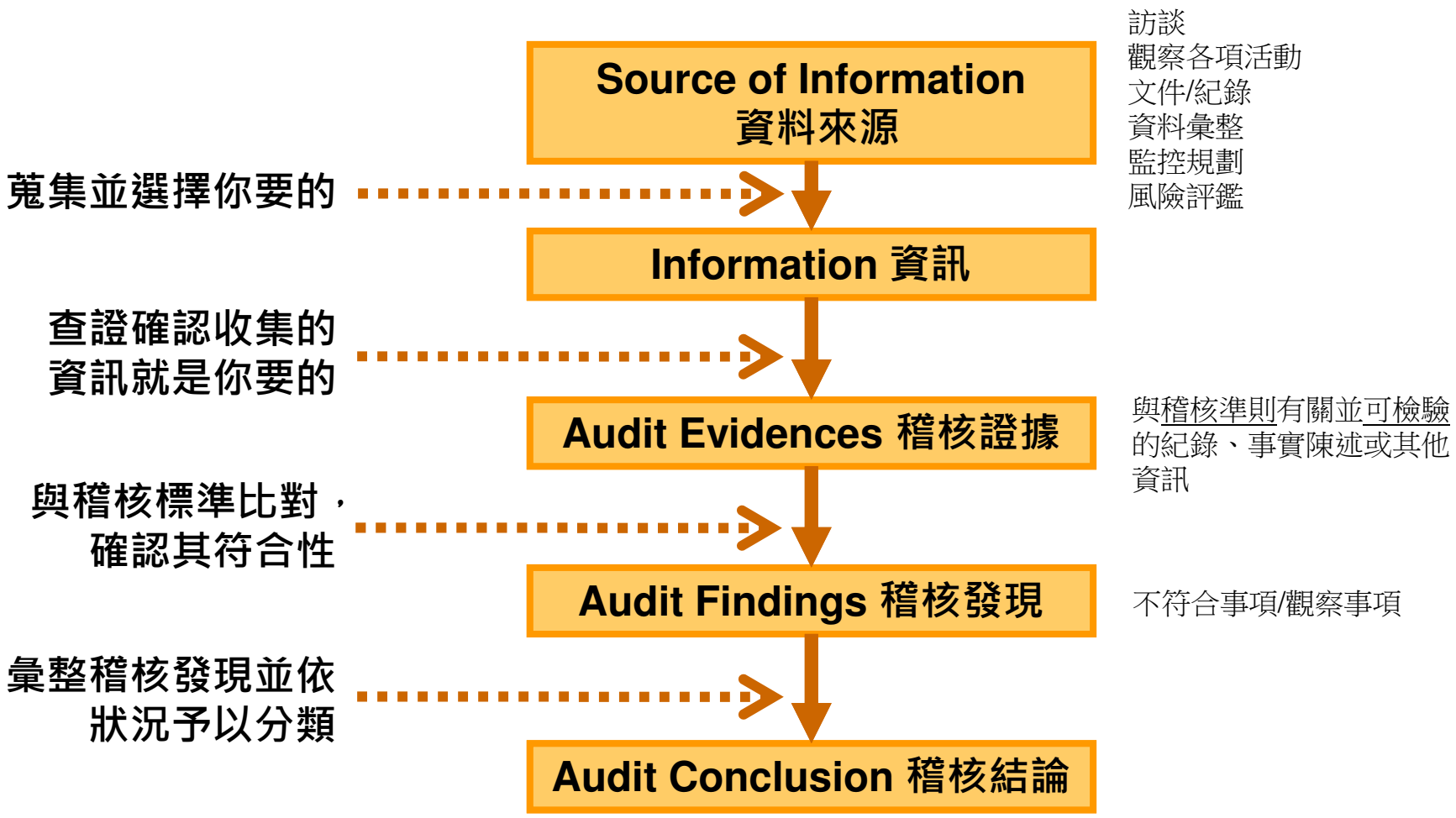
製作稽核工作文件

- **目的**
  - 確保達成稽核目標與範圍
  - 確保稽核的全部項目都已完成
  - 提供稽核員引導
- **考量**
  - 流程運作執行的地點
  - 相關程序
  - 使用的文件
  - 紀錄
  - BS 10012 標準的要求
  - 個人資訊管理系統的要求
  - 適用法規與法令

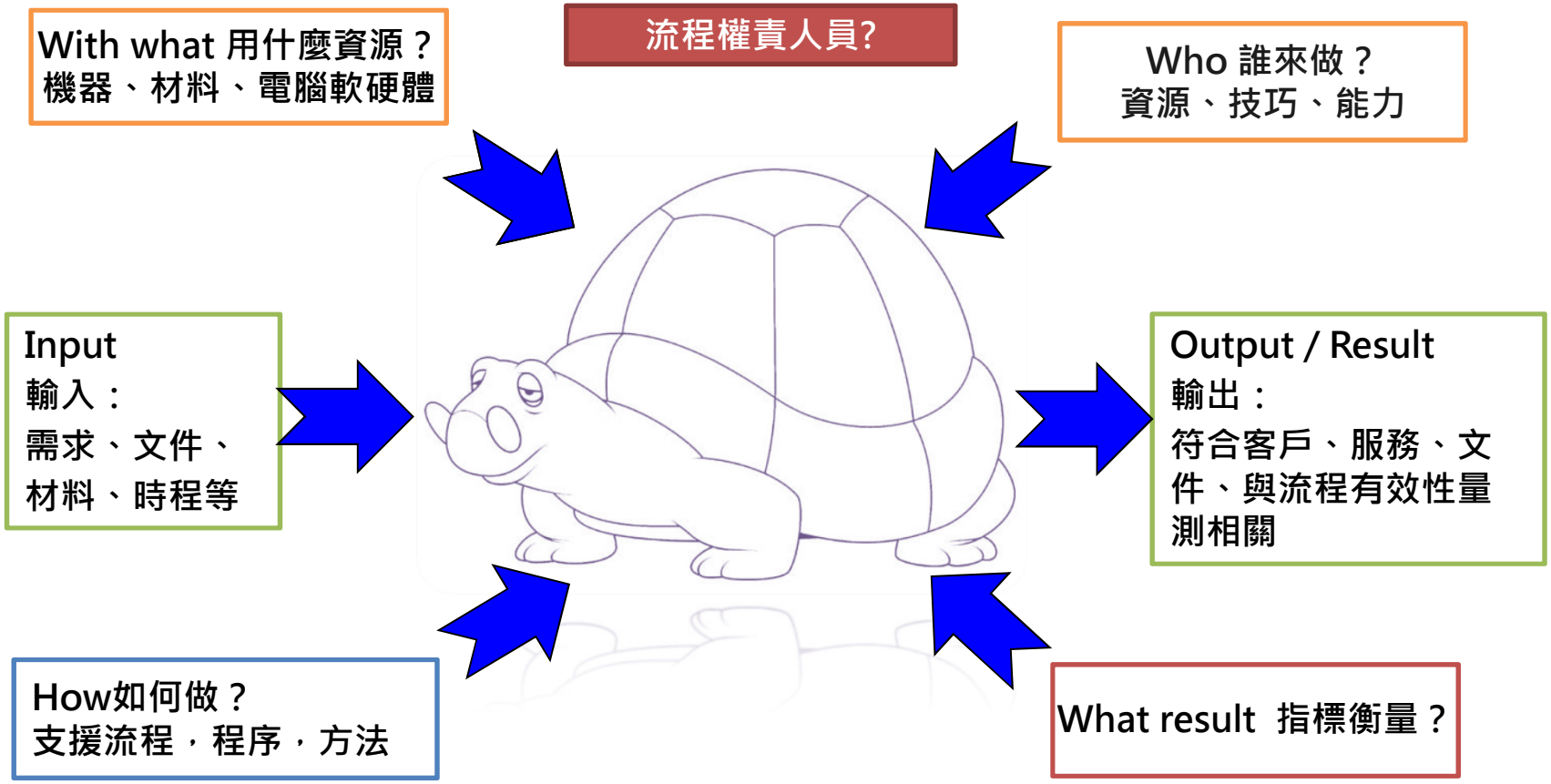
稽核執行方式

- **審查控制的基本概念，一般包括了審查程序、審查報告和審查後續行動**
- **執行個人資訊安全控制審查，稽核員可以應用三種審查方法，**
  - 檢查
  - 訪談
  - 測試

實地稽核流程證據蒐集方式



流程導向方法
PROCESS APPROACH



稽核之檢討

- 與被稽核人員討論發現事實。
- 複查查核表。
- 列出發現之不完備處。
- 決定不符合事項。
- 完成矯正行動需求表。

通常在稽核過程中與稽核完畢都可能實施

不符合事項

- 未能與組織適用的標準相吻合。
- 未能實施組織所規定的政策、程序書或其他指定文件的要求。
- 未能執行工作規定、法令、合約等規範。

No Requirement = No Nonconformance

稽核報告與跟催

- 簡報稽核發現
- 就稽核提出報告
- 完成稽核
- 矯正措施
- 矯正措施要求狀態表
- 管理審查
- 跟催與結案

稽核報告

- **結論：**
  - 符合的程度
  - 個人資訊管理系統的有效執行
  - 流程審查的管理能力，以確保個人資訊管理系統持續的適切與有效
- **內容**
  - 受稽單位名稱
  - 同意的稽核的目標, 範圍與排除項目
  - 稽核標準
  - 稽核日期, 地點
  - 稽核期間
  - 稽核發現
  - 組織代表
  - 稽核過程概要
  - 稽核發現的保密性宣告

完成稽核

All activities in the audit plan have been concluded, including distribution of audit report.

一當稽核計畫中所有的活動已經被執行, 包括分發稽核報告

驗證稽核案例分享

稽核發現—個人資訊管理
次要不符合事項

控制項

- 個資檔案同意書內未符合個資法告知事項
- 個資檔案個人資料流向與保存期限與實際作業未能符合
- 資檔案的保存與銷毀程序未符合要求
- 部分個資檔案未列入個人資料檔案清冊，盤點未落實
- 資料分享於非屬學校的第三人時未簽訂資料分享協議取得合法使用承諾
- 委外廠商涉及個資檔案合約要求未包含個資安全維護事項
- 個人資訊系統或資料庫帳號與權限控管未符合要求

稽核發現—個人資訊管理
觀察事項

管理體系

- 風險評估方法與處理計畫宜再強化
- 有效性量測宜更清楚呈現抽樣與量測證據，以及其矯正時效
- 利害相關團體與要求事項文件化紀錄宜再強化

控制項

- 宜釐清個資檔案資料筆數紀錄與實際保存數量不一致，強化檔案保存管理
- 個人資料檔案擁有者與管理者角色與權責宜加以釐清。
- 個人資料為外處理未發現依據要求進行監督，如簽署保密界結書
- 個人資料系統帳號權限的合適性與登入通行碼變更要求

矯正與預防流程

矯正與預防措施

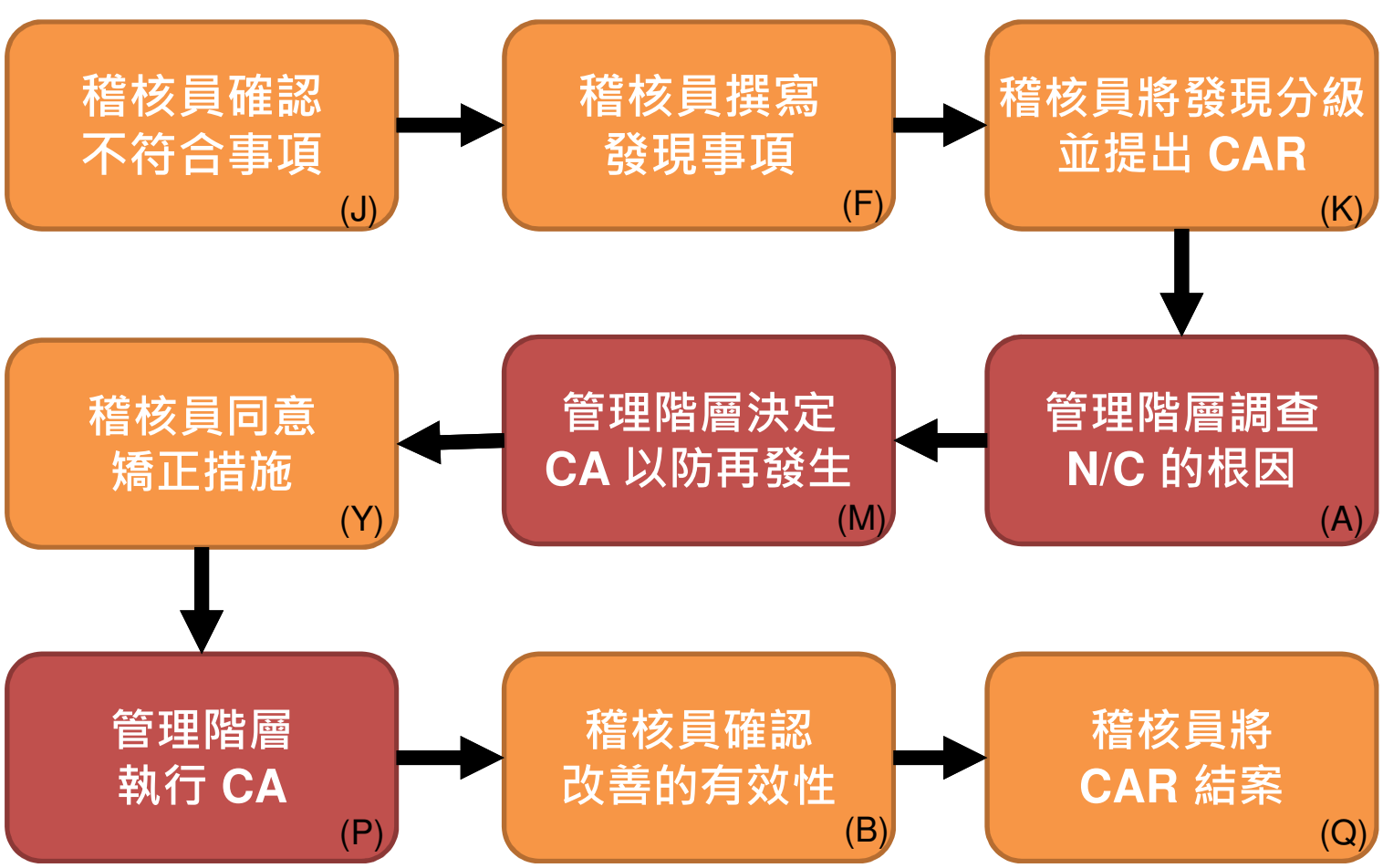
矯正措施

- a) 對不符合項目反應，採取行動控制並矯正；及處理其後果；
- b) 審查不符合項目、決定其原因；以及是否有類似項目存在，或可能發生；評估消除原因的行動需要，使其不再發生且不於他處發生：
- c) 實作所有所需行動；
- d) 審查所有所採取矯正措施之有效性；以及
- e) 必要時，則對PIMS進行變更。

預防措施

- a) 識別潛在不符合事項及其原因；
- b) 決定與實施所需之預防措施；
- c) 記錄所採取措施之結果並加以審查；
- d) 識別已變更之風險；及
- e) 確保所有應瞭解該潛在不符合原因及預防措施之人員皆被告知。

矯正措施典型處理循環


稽核員確認
不符合事項
(J)
稽核員撰寫
發現事項
(F)
稽核員將發現分級
並提出 CAR
(K)
管理階層調查
N/C 的根因
(A)
管理階層決定
CA 以防再發生
(M)
稽核員同意
矯正措施
(Y)
管理階層
執行 CA
(P)
稽核員確認
改善的有效性
(B)
稽核員將
CAR 結案
(Q)

解決不符合事項

管理階層應：

- 立即採取行動以矯正不符合事項
- 鑑別問題的根本原因
- 展開矯正措施以預防再發
- 執行並監控矯正措施

跟催與結案

- **跟催：**

  確定矯正措施的施行

- **結案：**

  矯正措施的查驗與允收

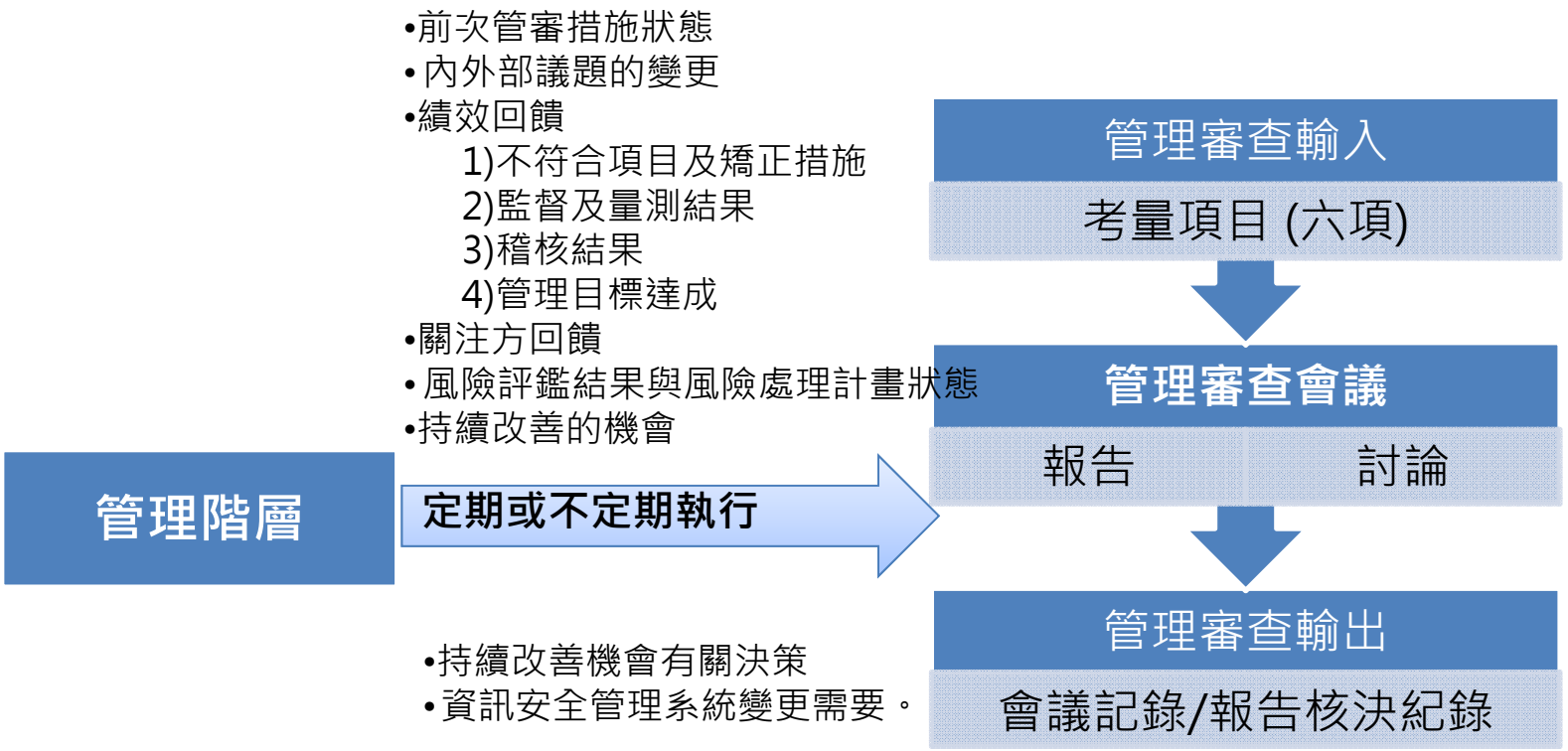
追蹤與結案之方法

- 審閱相關之文件。
- 拜訪被稽核區域。
- 稽核履行之客觀證據。
- 證明矯正之有效性。
- 記錄詳情。
- 不符合事項矯正預防措施結案。

管理審查

9.3 Management review 管理審查

- 最高管理階層應定期審查組織ISMS以持續確保適切性、合適性與有效性。



持續改進—管理階層審查

- **管理階層審查應考量：**
  - PIMS使用者的回饋
  - 員工對風險的識別及風險的提升
  - 稽核結果
  - 程序審查的紀錄
  - 技術的進步及/或更新結果
  - 執法單位對評鑑的正式要求
  - 抱怨的處理
  - 已發生之違反安全事件

持續改善

- **PIMS 有效性之持續改善，可透過：**
  - 建立個資管理文化
  - 從知情人士來的反應
  - 認知與教育訓練
  - 風險與安全評鑑
  - 法規與科技變化
  - 當事人的存取
  - 抱怨與申訴
  - 從安全事故中學習
  - 稽核結果
  - 矯正與預防措施

Q & A

THANKS FOR YOUR COOPERATION